February, 2019

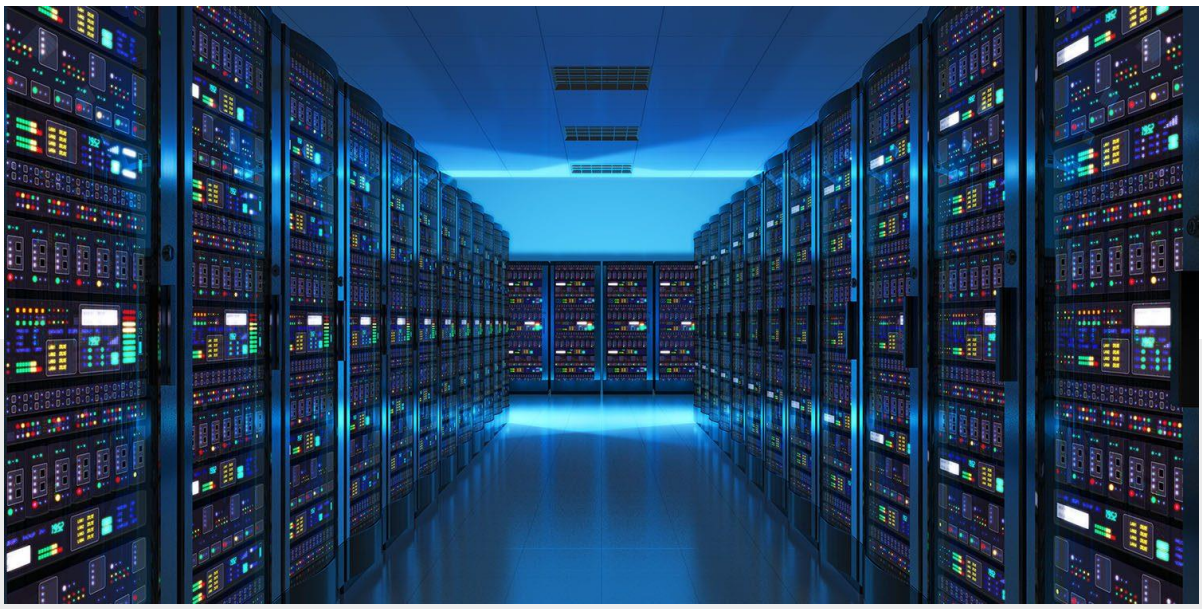
Renaissance IT Consulting, LLC

Technology Insider

BUILDING A DATA BACKUP AND DISASTER RECOVERY PLAN

The word “disaster” is widely used to describe a very terrible event – earthquake, tornado, hurricane, flood, wildfire – but the common result of any disaster is destruction. Destruction could include buildings, roads, power, transportation – and even include loss of life. To a business, disaster could also include the loss of the ability to do business, make or ship products, or meet customer demands. The cause of the disaster could be one of the events listed above – or even simpler – the loss of a critical business system or data. The system or data loss could be caused by hardware failure, failed patches or updates, data corruption, malware encryption, or simple programmer or developer error. At one of the companies I worked for, an SAP programmer mistakenly moved the wrong version of a code update from test to production, causing the corruption of plant inventories in all locations. The system was immediately taken off-line, the database restored to the latest backup from the night before – and inventories reset to the start of day numbers. The transaction log was re-applied, and the system was back and running with inventories at normal levels within 3 hours. Disaster averted due to the execution of a solid recovery plan.

So how do companies create such a plan? The steps are simple - the process takes time. Getting the business to participate in answering the questions is a key success factor to your plan. And after the data is gathered, researching and selecting the proper vendor or services will take time.



Step 1: Complete a Business Impact Analysis (BIA).

Ask the hard questions. What are the threats to your business? How likely are these threats to occur? How long – in units of time – can the business afford to be down. What is the Recovery Time Objective (RTO) for each critical system – the maximum tolerable length of time that a computer, system, network or application can be down after a failure or disaster occurs. Define the Recovery Point Objective (RPO) – is the maximum acceptable amount of data loss measured in time. It is the age of files that must be recovered from backup for normal operations to resume if a computer, system, network or application goes down. Consider the effect of lost productivity, missed sales, brand damage or lost progress.

Step 2: Identify Critical Data and Assets

It's important to know what assets and data must be brought back on-line immediately and what can wait. If you're an e-commerce business, maybe your EDI or customer facing website are most important. If you're a manufacturing business, maybe your shop floor control systems or shipping and receiving systems are highly critical. Remember, there will be limited funds to design and build fully redundant and restorable systems, so this step is important as you prioritize your spending.

Step 3: Decide on a Backup Location

Most companies design backup strategies which keep one copy local and one copy remote – and new faster disk-based backups are replacing off-site tape rotations. Choosing the back-up location must take into consideration – performance and failback times – and if remote, network performance to restore the files or systems. The cloud offers safe, reliable, versatile solutions – especially if you are running virtual servers. The cost of replicating production environments can be expensive – and should be considered as new systems are designed – not after a disaster.

Step 4: Research and Choose the Right Solutions

The completed DR plan will force the IT team to implement both hardware and software tools to successfully meet the objectives identified above. A consistent strategy across the enterprise allows business to leverage their investment in hardware, software and cloud services. Most vendor models include on-site disk hardware that replicates to a cloud or remote private data center environment – controlled by a single management console. Each vendor's secret sauce is different (how data is deduplicated, compressed or encrypted) and the speed to recover can be different – so each solution should be tested before buying. Key vendors here include Infrascale, ExaGrid, Veeam, Rubrik, Dell/EMC Data Domain, IBM, NetApp, and Veritas among many others. Note there are plenty of new players in this space with cloud DR options and many offer recovery-as-a-service.

Step 5: Test the Plan

DR tests are not fun. They can be disruptive to the business – but they are necessary. The test is very simple – take the system off line and test the restore/recovery/failover process. A good time to test the plan is right before major system updates during a scheduled downtime. In fact, backups should always be taken just prior to major system updates anyway – so this is a good time to test the recovery process. It will be well worth your effort.

Special note: The recent threats from ransom-seeking threat actors who send phishing emails which when clicked, encrypt user systems and then spread to systems on the network are forcing the hands of businesses to backup data regularly. Of course, all steps should be taken to block these emails and educate users, but this malware will infect your organization at some point. I've seen many companies implement backup/restore processes to combat these attacks. Also, tools from Trend Micro, Sophos, Kaspersky and Malwarebytes offer ransomware detect and block tools for servers.

Chuck Maiorana
Renaissance IT Consulting, LLC
Shelby Twp., MI 48315

248-274-4480
cwmaiorana@renaissanceitconsulting.com
www.renaissanceitconsulting.com